NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

MAR 14 2002

Ms. Laura L. S. Kimberly
Acting Director
Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408

Dear Ms. Kimberly:

As requested, we have completed the "Reports on Cost Estimates for Security Classification Activities." Ms. Christine Dozier in the Division of Administrative Services is the agency point of contact. She may be reached at (703) 292-7531 or via email cdozier@nsf.gov.

Sincerely,

Mary Lou Higgs
Acting Director
Division of Administrative Services

Attachment

Rec'd 3/25/02

2003 Security Costs Estimates Display

Name of Department/Agency: NATIONAL SCIENCE FOUNDATION

Reporting Categories	FY 2001 (Est. in $000s)	FY 2002 (Est. in $000s)	FY 2003 (Est. in $000s)
1. Personnel Security	50	52	52
2. Physical Security	5	5	5
3. Information Security (Sum of *a,b* & c below)	34.5	35	38.9
a. Classification Management	34.5	35	35.7
b. Declassification	0	0	0
c. Information Technology (Electronic Security)	0	0	3.2
4. Professional Education, Training and Awareness	.5	.5	.5
5. Security Management, Oversight and Planning	0	0	0
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	90	92.5	96.4
Totals: Full-Time Equivalents (FTE)	1	1	1

NARRATIVE:

National Science Foundation does not originate classified materials.

Rec'd Mar 17, 03

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

MAR 14 2003

Ms. Laura L. S. Kimberly
Associate Director for Policy
Information Security Oversight Office
700 Pennsylvania Ave, NW
Washington, DC 20408

Dear Ms. Kimberly:

As requested, we have completed the "Reports on Cost Estimates for Security Classification Activities." Ms. Christine Dozier in the Division of Administrative Services is the agency point of contact. She may be reached at (703) 292-7531 or via email cdozier@nsf.gov.

Sincerely,

Mary Lou Higgs
Director
Division of Administrative Services

Attachment

2004 Security Costs Estimates Display

Name of Department/Agency: NATIONAL SCIENCE FOUNDATION

Reporting Categories	FY 2002 (Est. in $OOOs	FY 2003 (Est, in $OOOs	FY 2004 (Est. in $OOOs
1. Personnel Security	52	52	53
2. Physical Security	5	5	6
3. Information Security (Sum of a,b & e below)	35	38.9	39.4
a. Classification Management	35	*35.7*	*36*
b. Declassification	0	*0*	*0*
c. Information Technology (Electronic Security)	0	3.2	3.4
4. Professional Education, Training and Awareness	.5	.5	.5
5. Security Management, Oversight and Planning	0	0	0
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	92.5	96.4	98.9
Totals: Full-Time Equivalents (FTE)	1	1	1

NARRATIVE: National Science Foundation does not originate classified materials.

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

March 17, 2004

Ms. Laura L.S. Kimberly
Associate Director for Policy
Information Security Oversight Office
700 Pennsylvania Avenue, NW
Washington, DC 20048

Dear Ms. Kimberly:

Subject: Report on Cost Estimates for Security Classification Activities

As requested, we have completed the "Reports on Cost Estimates for Security Classification Activities." Ms Christine Dozier in the Division of Administrative Services is the agency point of contact. She may be reached at (703) 292-7531 or via email cdozier@nsf.gov.

Sincerely,

Mary Lou Higgs
Director
Division of Administrative Services

Attachment

2005 Security Costs Estimates Display

Name of Department/Agency **National Science Foundation**

Reporting Categories	FY 2003 (Est. in $000s)	FY 2004 (Est. in $000s)	FY 2005 (Est. in $000s)
1. Personnel Security	52	53	55
2. Physical Security	5	6	6
3. Information Security (Sum of *a, b,* c & d below)	38.9	39.4	42.6
a. Classification Management	35.7	36	39
b. Declassification	0	0	0
c. Information Systems Security	0	0	0
d. Miscellaneous (OPSEC & TSCM)	3.2	3.4	3.6
4. Professional Education, Training and Awareness	.5	.6	1.5
5. Security Management, Oversight and Planning	0	0	0
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	96.4	98.9	105.1
Totals: Full-Time Equivalents (FTEs)	1	1	1

NARRATIVE: National Science Foundation does not originate classified materials.

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

March 23, 2005

J. William Leonard
Director
Information Security Oversight Office
700 Pennsylvania Avenue, NW
Washington, DC 20048

Dear Mr. Leonard:

Subject: **Report on Cost Estimates for Security Classification Activities**

As requested, we have completed the "Report on Cost Estimates for Security Classification Activities." Ms. Christine Dozier in the Division of Administrative Services is the agency point of contact. She may be reached at (703) 292-7531 or via email cdozier@nsf.gov.

Sincerely,

Mary Lou Higgs
Director
Division of Administrative Services

FY 2006 Security Cost Estimates Display

Name of Department/Agency: NATIONAL SCIENCE FOUNDATION

(Please use actual dollar figures instead of thousands.)

Reporting Categories	FY 2004	FY 2005	FY 2006
1. Personnel Security	53,000	55,000	55,000
2. Physical Security	6,000	6,000	4,000
3. Information Security			
(a.) Classification Management	36,000	39,000	41,500
(b.) Declassification	0	0	0
(c.) Information Systems Security for Classified Information	0	0	0
(d.) Miscellaneous (OPSEC & TCSM)	3,400	3,600	3,600
(e.) Information Security Subtotal *(sum of 3.a., 3.b., 3.c., & 3.d.)*	39,400	42,600	45,100
4. Professional Education, Training and Awareness	600	1,500	1,500
5. Security Management, Oversight and Planning	0	0	0
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6)	~~93,000~~ 99,000	99,100	101,600

NARRATIVE:

National Science Foundation does not have original classification authority.

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

March 27, 2006

J. William Leonard
Director
Information Security Oversight Office
700 Pennsylvania Avenue, NW
Washington, DC 20048

Dear Mr. Leonard:

Subject: **Report on Cost Estimates for Security Classification Activities**

As requested, we have completed the "Report on Cost Estimates for Security Classification Activities." Ms. Christine Dozier in the Division of Administrative Services is the agency point of contact. She may be reached at (703) 292-7531 or via email cdozier@nsf.gov.

Sincerely,

Mary Lou Higgs
Director
Division of Administrative Services

Security Cost Estimates Display

Name of Department/Agency: NATIONAL SCIENCE FOUNDATION

(Please use actual dollar figures instead of thousands.)

Reporting Categories	FY 2005	FY 2006	FY 2007
1. Personnel Security	31,914	55,000	55,000
2. Physical Security	6,000	4,000	4,000
3. Information Security			
(a.) Classification Management	39,000	42,898	42,898
(b.) Declassification	0	0	0
(c.) Information Systems Security for Classified Information	0	0	0
(d.) Miscellaneous (OPSEC & TCSM)	3,600	3,600	3,600
(e.) Information Security Subtotal *(sum of 3.a., 3.b., 3.c., & 3.d.)*	~~41,514~~ 42,600	46,498	46,498
4. Professional Education, Training and Awareness	1,500	1,500	1,500
5. Security Management, Oversight and Planning	0	0	0
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6)	~~80,928~~ 82,014	107,398	107,398

NARRATIVE:

National Science Foundation does not have original classification authority.

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

March 29, 2007

J. William Leonard
Director
Information Security Oversight Office
700 Pennsylvania Avenue, NW
Washington, DC 20048

Dear Mr. Leonard:

Subject: **Report on Cost Estimates for Security Classification Activities**

As requested, we have completed the "Report on Cost Estimates for Security Classification Activities". Ms. Christine Dozier in the Division of Administrative Services is the agency point of contact. She may be reached at (703) 292-7531 or via email cdozier@nsf.gov.

Sincerely,

Mary Lou Higgs
Director
Division of Administrative Services

Security Costs Estimates Display

Name of Department/Agency: NATIONAL SCIENCE FOUNDATION

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2006
1. Personnel Security	75,796.00
2. Physical Security	1,000.00
3. Information Security	
(a.) Classification Management	42,898
(b.) Declassification	0
(c.) Information Systems Security for Classified Information	0
(d.) Miscellaneous (OPSEC & TSCM)	1,716.00
(e.) Information Security Sub-Total *(Sum of 3.a., 3.b., 3.c., &3.d.)*	44,614.00
4. Professional Education, Training and Awareness	0
5. Security Management, Oversight and Planning	0
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6.)	121,410.00

NARRATIVE:

The National Science Foundation does not have original classification authority.

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

March 13, 2008

William J. Bosanko
Acting Director
Information Security Oversight Office
700 Pennsylvania Avenue, NW, Room 503
Washington, DC 20408-0001

Dear Mr. Bosanko:

Subject: **Report on Cost Estimates for Security Classification Activities**

As requested we have completed the estimate on costs for fiscal year 2007 security classification activities. Ms. Christine Dozier in the Division of Administrative Services is the agency point of contact. She may be reached at (703)292-7531 or via email cdozier@nsf.gov.

Sincerely,

Pat Bryant
Director
Division of Administrative Services

Enclosure

Security Costs Estimates Display

Name of Department/Agency: NATIONAL SCIENCE FOUNDATION

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2007
1. Personnel Security	84,500.
2. Physical Security	2,000.
3. Information Security	
(a.) *Classification Management*	44,032.
(b.) *Declassification*	0
(c.) *Information Systems Security for Classified Information*	0
(d.) *Miscellaneous (OPSEC & TSCM)*	1,226.
(e.) ***Information Security Sub-Total*** *(Sum of 3.a., 3.b., 3.c., & 3.d.)*	45,258
4. Professional Education, Training and Awareness	500.
5. Security Management, Oversight and Planning	0
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6.)	132,258.

NARRATIVE: National Science Foundation does not have original classification authority.

Security Costs Estimates Display

Name of Agency:
National Science Foundation

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2008
1. Personnel Security	64,638.
2. Physical Security	500.
3. Information Security	
(a.) Classification Management	48,302.
(b.) Declassification	0
(c.) Information Systems Security for Classified Information	0
(d.) Miscellaneous (OPSEC & TSCM)	1,300.
4. Professional Education, Training and Awareness	0
5. Security Management, Oversight and Planning	0
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(a,b,c,d), 4, 5, & 6.)	114,740.

NARRATIVE:

The National Science Foundation does not have original classification authority.

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

February 22, 2010

William J. Bosanko
Director
Information Security Oversight Office
700 Pennsylvania Avenue, NW
Washington, DC 20408

Dear Mr. Bosanko:

Subject: **Report on Cost Estimates for Security Activities for FY2009**

As requested we have completed the estimate on costs for fiscal year 2009 security classification activities. Ms. Christine Dozier in the Division of Administrative Services is the agency point of contact. She may be reached at 703-292-7531 or via email cdozier@nsf.gov.

Sincerely,

Pat Bryant

Pat Bryant
Director
Division of Administrative Services

Security Costs Estimates Display

Name of Department/Agency: NATIONAL SCIENCE FOUNDATION

Point of Contact (Name/phone number): CHRISTINE DOZIER (703)292-7531

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2009
1. Personnel Security	130,175.
2. Physical Security	500.
3. Information Security	
(a) Classification Management	49,375.
(b) Declassification	0
(c) Information systems Security for Classified Information	0
(d) Miscellaneous (OPSEC & TSCM)	1,500.
4. Professional Education, Training, and Awareness	0
5. Security Management, Oversight, and Planning	0
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(a), 3(b), 3(c), 3(d), 4, 5, &6)	~~181,500.~~ 181,550

NARRATIVE:

The National Science Foundation does not have origina classification authority.

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

March 11, 2011

William J. Bosanko
Director
Information Security Oversight Office
700 Pennsylvania Avenue, NW, Room
Washington, DC 20408

Dear Mr. Bosanko:

Subject: **Report on Cost Estimates for Security Activities for FY 2010**

As requested we have completed the estimate on costs for fiscal year 2010 security classification activities. Ms. Christine Dozier I the Division of Administrative Services is the agency point of contact. She may be reached at (7030292-7531 or via email cdozier@nsf.gov.

Sincerely,

Paul Perez
Acting Director
Division of Administrative Services

Security Costs Estimates

Department/Agency: NATIONAL SCIENCE FOUNDATION **Fiscal Year:** 2010

Point of Contact: (Name and phone number) Christine Dozier: (703) 292-7531

Reporting Categories (Please use actual dollar figures instead of thousands)

1. Personnel Security $73,000.00

(include clearance program, initial investigations, notional agency checks when used for basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification related activities)

2. Physical Security $500.00

(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification related activities)

3. Information Security

(only report costs associated with classification related activities)

(a) Classification Management $49,375.00

(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

(b) Declassification $0.00

(include resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive order or statute)

(c) Information Systems Security for Classified Information $69,147.00

(include resources used to protect information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

(d) Miscellaneous (OPSEC and TSCM) $65,726.00

(include personnel and operating expenses associated with these programs)

4. Professional Education, Training, and Awareness $0.00

(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification related activities)

5. Security Management, Oversight, and Planning $0.00

(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

6. Unique Items $0.00

(include department/agency-specific activities not reported in any of the categories listed above but are nonetheless significant and need to be included)

Total (sum of 1, 2, 3(a), 3(b), 3(c), 3(d), 4, 5, and 6) $257,748.00

Narrative: *provide a brief explanation of any significance difference between last year's and this year's cost estimates. Explain items entered into Block 6. Unique Items.*

Installation of equipment to meet NCSD 3-1 Secret and Top Secret communication requirements. The National Science Foundation does not have original classification authority.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: National Science Foundation	**Fiscal Year:** 2011

Point of Contact:
(Name and phone number) Michael J. Owczarzak, 703-292-8085

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$164,191.00
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$17.33
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$44,293.00
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$0.00
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$100.82
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$0.00
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$208,602.15

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: National Science Foundation	**Fiscal Year:** 2012

Point of Contact:
(Name and phone number) Michael J. Owczarzak, 703-292-8085

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$136,929.00
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$0.00
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$1,127.25
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$0.00
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$91.32
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$0.00
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$138,147.57

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

In FY 11 there was a full time staff member (GS-6) supporting the Classified National Security Information protection program. In FY12, these duties were switched to collateral duties for two occupational series 0080 Security Administrators (GS13, GS-14). This change in program administration responsibility accounts for the decrease in reported resources in Block 8 between FY11 and FY12.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: National Science Foundation	**Fiscal Year:** 2013

Point of Contact:
(Name and phone number) Michael J. Owczarzak, 703-292-8085

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$178,610.00
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$10,790.00
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$2,839.58
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$0.00
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$161.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$1,388.06
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$655.28
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$194,443.92

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Item 1 increased approximately 30% due to changes in the agency's policies for on-boarding contractors resulting in a higher proportion of MBIs rather than previously accomplished NACIs.

Item 2 increased because of maintenance on GSA-approved storage containers.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: National Science Foundation | **Fiscal Year:** 2014

Point of Contact:
(Name and phone number) Jerene Shaheed 703-292-7562

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$262,630.00
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$3,591.00
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$14,362.00
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$0.00
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$895.00
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$0.00
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$281,478.00

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Agency purchased two GSA-compliant safes, each with four individually lockable drawers.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: National Science Foundation	**Fiscal Year:** 2015

Point of Contact:
(Name and phone number) Jerene Shaheed, Head, Security & Emergency Management, 703-292-7562

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$115,000.00
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$12,854.28
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$0.00
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$0.00
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$3,500.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$45,000.00
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$0.00
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$176,354.28

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

The significant decrease over FY2014 expenditures of ($105,123.72) illustrates implementation of the Agency's strategic plan for improving security capability throughout all facets of operations. Cat 1: declined as the Agency continued to review needed eligibilities and position descriptions. Cat 2: Increased dues to security systems improvements. Cat 3: Declined due to FY14 improvements Cat 6: Slight increase to due training in surveillance detection Cat 7: Increased as result of Agency-wide emphasis on security aware.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: National Science Foundation	**Fiscal Year:** 2016

Point of Contact:
(Name and phone number) Jerene Shaheed, Head Security & Emergency Mgt., 703-292-7562

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$69,322.00
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$0.00
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$0.00
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$600,000.00
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$1,040.00
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$0.00
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$670,362.00

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

The significant increase over FY2015 expenditures reflects overall enhancement of the Agency's security program, CAT 1: Incurred as a result of personnel security investigations and periodic re-investigations. CAT 2: Protective Security Officers secure the perimeter of the building and no specific internal secure areas. Per the tasking memo, this amount is not reported. CAT 3: No amplification required. CAT 4: No amplification required. CAT 5: Provides for contract assets to fully manage Agency COMSEC program. CAT 6: No amplification required. CAT 7: Incurred as result of Agency wide emphasis on security

The significant increase over FY2015 expenditures reflects overall enhancement of the Agency's security program:

CAT 1: Incurred as a result of personnel security investigations and periodic re-investigations.

CAT 2: Protective Security Officers secure the perimeter of the building and no specific internal secure areas. Per the tasking memo, this amount is not reported.

CAT 3: No amplification required.

CAT 4: No amplification required.

CAT 5: Provides for contract assets to fully manage Agency COMSEC program.

CAT 6: No amplification required.

CAT 7: Incurred as result of Agency-wide emphasis on security awareness.

CAT 8: No amplification required.

CAT 9: No amplification required.